Follow us On Twitter

Happy New Year !

February 2016 Issue

DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION

DTI *e*Security News — Mobile Edition

Connecting in the New Year

Many of us received or purchased new mobile devices during the holidays. Now more than ever, smartphones and tablets are the "go to" devices for all sorts of daily tasks, both business and personal. As helpful as the mobile machines are, they are also targets for criminals, both virtual and real. When using your mobile device for banking, business, or just fun, you should always make safety and security a priority.

Many of today's devices offer advanced levels of security such as touch, facial and voice recognition. It's important to explore the security features of your specific device.

Ways to Reduce Your Risk

Your device and your data are important and need to be protected. Here are examples that increase risk:

- Carrying both your business and personal information on the same device
- Connecting to unsecured public Wi-Fi
- Ignoring basic security controls, such as not setting device passcodes
- Malicious mobile app downloads from untrusted sources
- Use of Social Networks
- Using weak passwords for email and online payment and banking apps

Visit the DTI eSecurity website for previous issues of eSecurity Newsletters

Consider an Antivirus App

Viruses may be a more limited problem on smartphones and tablets, but they do exist. So do antivirus apps for helping you deal with them. Do you use them? Here are a few to consider:

- **Avast**
- **AVG**
- **Malwarebytes**

For more information, go to DTI's cyber security website, digiknow.delaware.gov.

Keep a Clean and Lean Device

It is not expensive or difficult to protect your mobile devices. Here are some tips on how to keep your devices safe:

1. **Keep your software updated.** This is one of your first lines of defense. Patches will help keep your device safe.
2. **Use strong passwords for your apps.** Make sure to use a combination of at least 10 characters, letters (upper and lower case), numbers and special characters.
3. **Keep your devices locked when not in use.** Require a passcode to unlock your device. On most devices, passcodes can be configured to be required after a set time of inactivity and at startup.
4. **Be mindful of the apps you are using.** Be very selective in which apps you download. Remove apps that you no longer use.
5. **Disable autofill.** If your mobile device automatically fills in passwords and login information, turn this feature off.

Questions or comments?
Email us at eSecurity@state.de.us